IN THE UNITED STATES PATENT AND TRADEMARK OFFICE (DO/US)

International Application No. PCT/GB98/02881

International Filing Date: 24 September 1998

Title: A DATA ENCRYPTION SYSTEM FOR INTERNET COMMUNICATION

Applicant for US: John Wolfgang HALPERN

Attorney's Docket: HALJW/102/PC/US

Box PCT
Commissioner for Patents
Washington, DC 20231

Sir:

Please commence the United States National Processing of the above-identified international application.

WE HEREBY REQUEST IMMEDIATE EXAMINATION UNDER 35 U.S.C. 371(f).

The following items are enclosed:

(1) A check in the amount of $430.00 to cover the national fee, which has been calculated as follows:

Basic fee (Filing with EPO search report 37 CFR § 1.492(a)(5)):	$430.00
Applicant claims small entity status	
Independent claims in excess of 3 (0 x 80):	0.00
Claims in excess of 20 (0 x 18):	0.00
No multiple dependent claims presented:	0.00
Total:	$430.00

EXPRESS MAIL Mailing Label Number EL721435571US

Date of Deposit: March 19, 2001

The commissioner is hereby authorized to charge any additional filing fees which may be required to complete the requirements for national processing of the above-identified international application to Deposit Account 16-2563.

(2) Signed Inventor's Declaration.

(3) Copy of the International Application Published Under the PCT

(4) Copy of annexes to the International Application

(5) Preliminary Amendment, which should be entered before calculating the filing fee.

(6) EPO Search Report

(7) Petition Under 37 C.F.R. § 1.137(b)

The application to be examined in the United States consists of the enclosed amended International Application after the enclosed Preliminary Amendment has been entered.

Respectfully submitted,
JOHN WOLFGANG HALPERN et al

By____________________
Guy D. Yale
Registration No. 29,125
Attorney for Applicant
Alix, Yale & Ristas, LLP
750 Main Street
Hartford, CT 06103

Date: March 19, 2001

Telephone: (860) 527-9211
Facsimile: (860) 527-5029

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

International Application No.: PCT/GB98/02881

International Filing Date: 24 September 1998

Title: A Data Encryption System for Internet Communication

Inventor: John Wolfgang HALPERN

Attorney Docket No: HALJW/102/PC/US

Box PCT
Commissioner for Patents
Washington, D.C. 20231

Sir:

PRELIMINARY AMENDMENT

Applicant requests entry of the following preliminary amendment prior to calculation of the filing fee. Please amend the above-identified international application as follows:

In the claims:

Claim 3, line 2, delete "or 2".

Claim 7, line 2, delete "or 6".

9. (Amended) An encryption and automatic key renewal system for confidential e-mail as in [any of the preceding claims] claim 1, comprising:

(a) a stored key verification and key exchange module (1),

(b) a Pseudo Random Key Generator (2),

(c) a system of logic circuit elements and interconnections between them,

(d) a programmable counter (4),

(e) an open-ended shift register with parallel bit outputs (7),

(f) a pseudo-random Data Generator (11) for supplying surplus data bits,

(g) a one clock-pulse delay circuit which delays real data bits (incoming and outgoing in affecting the machine state or algorithm status), and

(h) a serial buffer system (18) for accepting work station data and to pass them to the algorithm in accordance with the instant state of the algorithm.

EL721435571US

11. (Amended) An encryption and automatic key renewal system as [claimed in any preceding] in claim 1, wherein said data to be encrypted is encrypted using a variable word length encryption system, wherein the data output from the encryption system comprises random data bits and real data bits, said real data bits being transmitted at a randomly varying rate, according to the key being used by said e-mail station.

15. (Amended) An encryption and automatic key renewal system for confidential e-mail as claimed in [any of claims] claim 1 [to 11, 13 or 14], wherein the encryption process is determined by an algorithm embodied in a microelectronic chip and wherein this process is not rigidly predetermined but continually influenced and modified

(a) by the parallel bit outputs of a revolving encryption key register, and

(b) by some but not all the clear bits of the data inputted to the said algorithm circuit for encryption or outputted from the said algorithm circuit after decryption.

Please add the following new claims:

--18. An encryption and automatic key renewal system for confidential e-mail as claimed in claim 13, wherein the encryption process is determined by an algorithm embodied in a microelectronic chip and wherein this process is not rigidly predetermined but continually influenced and modified

(a) by the parallel bit outputs of a revolving encryption key register, and

(b) by some but not all the clear bits of the data inputted to the said algorithm circuit for encryption or outputted from the said algorithm circuit after decryption.

19. An encryption and automatic key renewal system for confidential e-mail as claimed in claim 14, wherein the encryption process is determined by an algorithm embodied in a microelectronic chip and wherein this process is not rigidly predetermined but continually influenced and modified

(a) by the parallel bit outputs of a revolving encryption key register, and

(b) by some but not all the clear bits of the data inputted to the said algorithm circuit for encryption or outputted from the said algorithm circuit after decryption.--

REMARKS

The claims have been amended to eliminate any multiple claim dependencies.

Please enter the preceding preliminary amendment prior to calculation of the filing fee.

Respectfully submitted,
John Wolfgang HALPERN

By____________________
Guy D. Yale
Registration No. 29,125
Alix, Yale & Ristas, LLP
Attorney for Applicant

Date: March 19, 2001
750 Main Street
Hartford, CT 06103-2721
(860) 527-9211
Attorney's Docket: HALJW/102/PC/US

CLEAN COPY OF AMENDED CLAIMS 3, 7, 9, 11, 15, AND NEW CLAIMS 18 AND 19 APPLICATION NO.: PCT/GB98/02881

3. An encryption and automatic key renewal system for confidential e-mail as in claim 1, comprising means for recognizing the legitimacy of a server station by a calling e-mail station, comprising

(a) means for sending to the server station the address code associated with the e-mail station's encrypting key;

(b) means for using the address to assist the server station in obtaining the calling station's encryption key;

(c) the server station comprising equipment to encrypt the key encryption number with itself;

(d) the server station also comprising means to send the encrypted key to the e-mail station;

(e) the e-mail station comprising means for decrypting the received key, using its own key and placing the result into a comparator register, and means for determining if the compared numbers are equal for informing the server station accordingly.

7. An encryption and automatic key renewal system for confidential e-mail as in claim 5, wherein the algorithms used for the encrypting process produce word-bit configurations consisting of more than 8 bits and less than 16 bits per word transmitted, and the bit number per word is continually changing.

9. An encryption and automatic key renewal system for confidential e-mail as in claim 1, comprising:

(a) a stored key verification and key exchange module (1),

(b) a Pseudo Random Key Generator (2),

(c) a system of logic circuit elements and interconnections between them,

(d) a programmable counter (4),

(e) an open-ended shift register with parallel bit outputs (7),

(f) a pseudo-random Data Generator (11) for supplying surplus data bits,

(g) a one clock-pulse delay circuit which delays real data bits (incoming and outgoing in affecting the machine state or algorithm status), and

(h) a serial buffer system (18) for accepting work station data and to pass them to the algorithm in accordance with the instant state of the algorithm.

11. An encryption and automatic key renewal system as in claim 1, wherein said data to be encrypted is encrypted using a variable word length encryption system, wherein the data output from the encryption system comprises random data bits and real data bits, said real data bits being transmitted at a randomly varying rate, according to the key being used by said e-mail station.

15. An encryption and automatic key renewal system for confidential e-mail as claimed in claim 1, wherein the encryption process is determined by an algorithm embodied in a microelectronic chip and wherein this process is not rigidly predetermined but continually influenced and modified

(a) by the parallel bit outputs of a revolving encryption key register, and

(b) by some but not all the clear bits of the data inputted to the said algorithm circuit for encryption or outputted from the said algorithm circuit after decryption.

18. An encryption and automatic key renewal system for confidential e-mail as claimed in claim 13, wherein the encryption process is determined by an algorithm embodied in a microelectronic chip and wherein this process is not rigidly predetermined but continually influenced and modified

(a) by the parallel bit outputs of a revolving encryption key register, and

(b) by some but not all the clear bits of the data inputted to the said algorithm circuit for encryption or outputted from the said algorithm circuit after decryption.

19. An encryption and automatic key renewal system for confidential e-mail as claimed in claim 14, wherein the encryption process is determined by an algorithm embodied in a microelectronic chip and wherein this process is not rigidly predetermined but continually influenced and modified

(a) by the parallel bit outputs of a revolving encryption key register, and

(b) by some but not all the clear bits of the data inputted to the said algorithm circuit for encryption or outputted from the said algorithm circuit after decryption.

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
H04L 29/06

A3

(11) International Publication Number: WO 99/16199

(43) International Publication Date: 1 April 1999 (01.04.99)

(21) International Application Number: PCT/GB98/02881

(22) International Filing Date: 24 September 1998 (24.09.98)

(30) Priority Data:

9720478.8	25 September 1997 (25.09.97)	GB
9820824.2	24 September 1998 (24.09.98)	GB

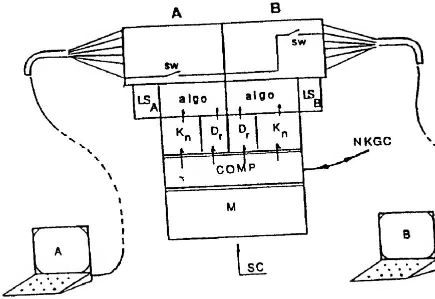
(81) Designated States: PL, PT, RU, SE, US, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With internationol search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(88) Date of publication of the international search report: 21 October 1999 (21.10.99)

(71)(72) Applicant and Inventor: HALPERN, John, Wolfgang [GB/GB]; 15 Jordan Court, Imgram Crescent W., Hove, East Sussex BN3 5NU (GB).

(54) Title: A DATA ENCRYPTION SYSTEM FOR INTERNET COMMUNICATION



(57) Abstract

Two versions of a variable word length encryption method are discussed adapted for providing the means for long-term confidential transmission of printed characters, pictures, and voice dialogues over the telephone lines or the internet.

A Data Encryption System for Internet Communication

There is a general concensus that serious use of the internet potential for the needs of Commerce and Industry requires a 100% long-term effective system for protecting privacy of the interchanges.

Several aspects apart from privacy would be important in making a choice of the technique. It would have to be suitable for all digital transmissions, irrespective of the coding employed. The same encryption system should be workkable for lettered, audible or visual messages. Also, the time of processing the data should preferably not add more than 80% to the time for transmitting the same data in the clear form. Furthermore, no time should be spent on looking up directories for keys or other procedure rules.

EP-A-0738 058 discloses a system for the secure distribution of encryption keys using a key management device attached to each user's encryption machine, containing a list of secure communication partners and their respective encryption keys. If the desired addressee data is not found in the local data list, the device connects to a secure key distribution centre which is protected by encryption using the public key method.

Kazue Tanake et al: "Key Distribution System for Mail Systems using ID-Related Information Directory", Computers and Security International Journal Devoted to the Study of Technical and Financial Aspects of Computer Security, vol. 10, no. 1 (1991-02-01), pp 25 - 33, ISSD 0167-4048, discloses a key distribution system which uses a public directory, which contains each user's ID-related information. A sender generates a key and key information which depends on the receiver, and sends the key information along with the encrypted message.

The objectives of this patent application follow from what has just been said:

- to create for owners of PC's certain supplementary components easily added with the result of replacing registered and high-priority mail transmissions by a less expensive and faster track.protected against breach of confidentiality.
- to reduce the need for personal trustworthiness and to replace it by trustworthiness of the provisions of the system.
- While the idea of "trusted third parties" is appropriate where Government interests are directly involved, the many contingencies that arise when applied to all communications would strain an already overburdened legal system. In contradistinction, the here proposed method would save trustworthy server stations from slipping into arbitrariness, favoritism and self-serving bureaucracy. At the same time it would open a clear route for observers at Govenment level to use their authority of sampling messages in the interest of crime prevention and to do so even for longer periods if and when properly authorized and reasoned for in exposès open for public inspection within six years.

This paper will outline the technical platform for accomplishing the above sketched objectives, with the further provision that its service be available to everyone at a relatively low extra cost over and above the cost of using internet communication.

The said 'technical platform' constitutes a system resting on two main pillars, namely

(a) an algorithm which generates variable wordlength data scrambling

(b) a hierarchic system of key distribution (e.g. a regulated method for ageing and then eliminating keys)

In accordance with a first aspect, the present invention provides an encryption and fully automatic key renewal system for confidential e-mail communication, comprising at least two e-mail stations linked to a communication system; the encryption and automatic key renewal system comprising:

a key generation centre (NKGC) for the generation of random keys for the use of said at least two e-mail stations;

means for the periodic renewal of the keys used by said at least two e-mail stations; and

means for scrambling or encrypting data to be transmitted, using said keys; and

local server stations which store and update said random keys generated in said key generation centre; characterised in that

said local server stations store said keys in a look-up table, each key being associated with an address code and each address code having associated data indicative of the age of said key at any time and to classify the age relative to the age of other keys in use at any given time; and

each said server station including means adapted to issue, prior to each confidential e-mail communication from said at least two e-mail stations, a new key to the sending e-mail station, as the key to be used by said station for scrambling or encrypting the data to be transmitted;

wherein said look-up table means stores a fixed number of encryption key numbers conjointly with their respective access addresses in a shift register-like memory structure wherein the said fixed group of key numbers and said addresses can be moved at quasi randomly arranged times from a younger to an older position the youngest position serving as an entrance point for a new number supplied by the said key generation centre, and the oldest number being relegated to an inactive and reserved position outside the said fixed number or group of encryption keys.

In accordance with an second aspect, there is provided an encryption and automatic encryption key renewal system for confidential e-mail communication, comprising at least one e-mail station linked to a communication system; said system comprising a pseudo-random data generator; characterised by a key generation system and an encryption circuit, said key generation system automatically providing said e-mail station with a new encryption key before each e-mail communication, and wherein the output of said pseudo-random data generator is mixed with the bit levels of outputs of said encryption circuit and with clear bit levels of said input data, according to said key, so as to diffuse any pattern such as may be recognised in the expanded data words.

In place of a lengthy explanation, we begin by referring to Figure 4 which illustrates the idea of variable word length text transformation. It will be clear that computerised scanning of the encrypted text will in this case have no prospect of providing any clue.

Figure 5 shows a functional block diagram of the encryption/decryption hardware. In early implementations, a 16 bit shift register was used (block SR) with simple output to input connection. The encrypted output resulting from such an arrangement showed a certain periodicity if the clear text consisted of the binary representation of a single letter, for example the letter 'a' in unchanging repetition. This revealed the potential for a certain weakness of the method unless steps are taken to overcome this possible point of attack for a hacker. In present designs we use a 31 bit shift register as the basis for a pseudo random data generator wherein the periodicity is vastly (pattern recurrance only once every 2,14 billion different combinations) reduced. In addition, further measures are taken to begin each message with an undefined length of meaningless text. That text is not delivered in clear by the algorithm. For the user it constitutes simply a few seconds waiting time added to the setting up time. One method of achieving this will be explained in conjunction with Figures 3,4 and 8.

Returning to the description of Fig. 5, paralell outputs from the shift register are connected to various logic elements under the heading LOGIC CONTROL. This comprises for example, a programmable counter, several flip flops and bistables and various gates. Some of the logic control elements are also exposed to inputs of the logic levels of the real data, both outgoing or incoming. These data are applied with a delay of one full clock pulse duration. This is done in the squares named 'bit delay'. The encrypted text on line l_2 is derived from an OR gate into which alternately pass bit elements from the real data and from the Random data generator RDG, respectively a, by real data modified,output from said generator. Encrypted data received are descrambled by action of the Logic Control group, in a single AND gate.

Figures 6 and 7 explain how it is possible to have 8 - 10 simultaneously valid keys and how they are weighted in a number ageing process. Figure 8 shows a functional block diagram of an LSI chip such as would be capable of carrying out data encryption at a high clock rate suitable for any communication network and would provide added security over and above the basic scheme of Figure 5.

Detailed Discussion of the Drawings

FIG. 1 shows two personal computers or communication work stations using a fixed secret key, or using a program permitting one of the stations to utilize the encryption key of the other.

FIG. 2 illustrates a situation where the official key employed within an organisation is not normally used for the actual encryption/decryption of data. If for example station A represents the word processor in a secretarial pool of one company, and station B the processor office in another company, And the message sender has a small computer in his office A_p wishing to send a confidential message to â particular person having a computer B_p , then the procedure would be as follows:

(a) The secretary at A will type into the word processor A a statement from Mr. A_p in clear language and put it on disk.

(b) Next, the secretary agrees with A_p to display on the window of A_p the text as written for approval or amendments.

(c) When approved, A_p will contact the secretary at A over the phone to prepare internet connection with the communication of office at B.

(d) When communication is established, the secretary rings A_p to report 'ready'.

(e) The executive at A_p now types his private password ppw into his keyboard thereby transmitting it to work station A where the instruction code tells the computer to deduct (or add) the password number, or a multiple thereof, from the encryption key of the organisation.

(f) Once this is done a green light informs the secretary that the clear text derived from the disk is to be moved through the encryption algorithm and out into the internet.

(g) The encrypted message is taken on disk at computer unit B. It cannot be read by staff.

(h) When executive B_p returns to his office, he will find a light signal indicating that he has a personal message. Accordingly, he will enter the agreed pass word ppw on his computer keyboard together with the instruction of deducting it from the common general key. After that, the decrypted message will appear on the screen B_p.

It would be technically possible to provide the Managing Chief in each company with an automatic printout of all personal messages, to enforce the sharing of confidential information.

Since the encryption system here expounded is not primarily determined by mathematical conversions, and therefore all numbers are equally suitable, it would suffice if the executives concerned are told that they must have a six-digit ppw. Knoledge of agreed passwords may therefore be limited to the parties themselves.

FIG. 3 shows the structure of a Service Center SC for almost fully automatic connection service to clients wishing to send messages required to remain confidential. Fig.3 shows again a workstation A in one locality and another workstation in a remote locality but using the same equipment. The central server station consists of two sections (A & B). These sections comprise channel switching section sw, switch control sections LS_A or LS_B; Two algorithmic sections virtually identically with those shown for example in Fig. 8; In each section is also a key register for storing a key K_n and a random text data holding register D_r. Below is a computing section COMP, and below that a memory of past transactions, M. The computer unit COMP has a preferably direct link with a National Key Generator Center NKGC. Where a direct link is not available, a switched connection with NKGC will do because no clear data are passed through this link. (see also Fig. 6) The process prior to A sending a confidential message to B, can be reported in ten steps.

(1) station A dials the local Service Center (SC) and immediately thereafter dials also the number of the desired receipient B.

(2) Station A gets indication that connection is made

(3) prompted by (2), section A receives from station A the address code for identifying the key held at present by station A. (see address reg., fig.7).

(4) section B of SC calls station B.

(5) Station B responds by sending its address in clear

(6) using the two address numbers from A and B, the SC looks up from a memory table similar to that of Fig. 7 the at the time valid secret key numbers. Section A of SC extracts the key nr. for station A, inserts it into the algorithm (algo) thereby encrypting K_A by K_A and sends it to station A for verification. - Section B of SC proceeds likewise with station B. (the table is stored in section COMP, and is periodically updated from the national key generator centre, see Fig. 6).

(7) A and B receive the encrypted keys K_A' and K_B' respectively, decrypt them with their respective K_A and K_B keys, and if any station cannot verify it sends to the respective section of SC a repeat request. If this also fails .. a 'failed' signal in clear goes to both stations.

(8) With both comparisons correct, the SC proceeds to obtain from its COMP section an alternative key number K_C which section A encrypts with K_A, and section B encrypts with K_B, and sends these numbers to stations A and B respectively where they are decrypted and entered into their key registers, substituting their earlier keys.

(9) Stations A and B send out K_C' to the respective sections of SC where they are compared to test equality.

at this point both stations would be ready to communicate. The time lapse so far (after the initial dialling by station A) would be less than 4 seconds. To improve security further a further step is adding a few seconds to the setting up procedure:

(10) The Computer Resource Unit COMP supplies to the operative sections a random number called D_r where it is entered into a register connected for generating through re-circulation a fairly large pseudo random number. This number is continually passed through tha algo sections of SC,and the output is//sent to stations A and B where they are decrypted and continually passed through a comparator register being only a few bits (5 - 12) long. Paralell outputs from this register are continually compared with a similar number of selected paralell bit outputs from the larger, in the opposite sense rotating, key register. Whenever all the bit positions of the static bit comparator are at the strobing moment equal, a pulse is released both in the stations A and B and in the Server Center SC internally which stops the D_r bit generator and establishes in the switching sections sw a direct connection between A and B.

It should be noted that the true time distance in terms of real data clock pulses could not be determined by a hacker and therefore no conclusion be drawn as to the number structure of the initial key in the key register of the algorithm. This is because the variable word length encryption applies also to the D_r data stream transmission.

Figure 4 illustrates the nature of an encrypted message consisting as it does of an initial phase of random data the length of which cannot be externally detected, and a transmission phase consisting of a quasi-random mixture of real data bits and random bits - all in a single undivided string of bits giving no clue where one word begins or ends. There is thus no reference points against which an analyst might be able to study the bit sequences.

Figure 5 has already been adequately dealt with on page 2

FIGURE 6 explains the role of the N K G C (national key generator center). In that Center the K_n numbers with their address allocations, and also the D_r numbers are generated and the protocol for the transfer of these numbers to head offices of various kind is observed. The management of the Center would be limited to determining the optimum rate at which updates for new numbers should be made. This would be set responsive to the performance of the system as a whole as reported by supervisors. Performance reports from head offices such as Bk (banks) or TR (transport organisations) or SC's (service centers for confidential communications) would be studied by supervisors and appropriate responses formulated. Management would have no access to actual key numbers. When a station mal-performs, its encryption module is detached and sent to the factory,and replaced by a factory-new one.

It is here suggested that both systemwise and with respect to the encryption module IC, the here explained confidential message system may be used also in bank transaction as also in remotely issued travel passes and routing instructions.

FIGURE 7. This table surveys the position changes of a number which ranges from a nascent phase to an active, semi-active, and finally abandoned phase. The numbers are classified in terms of age. The active number range comprises in this example five ageing positions, and so does the semi-active range of numbers. If each column segment represents the time span of, say, one week, it would take ten weeks for a number to travel from the nascent region through the active and semi-active region, in order to exit into the for normal use inaccessable abandoned region.

Once an address is allocated to a number, the two numbers remain associated during their migration through said regions.

Both active and semi-active numbers are valid numbers, and are therefore accepted by terminals and server stations for commencing a communication. However, either right at the beginning or after completion of the communication event, an older active number is substituted by a younger one, or any semi-active number is substituted by any number from the active region. If an internet station, or an IC card - through non-useage over a longer period of time - has in its encryption algorithm a number which at the time of re-use belongs to an abandoned number, it would be necessary to make contact with certain supervisory organs which have at their disposal access to a central register which keeps a record of numbers abandoned in the past. Such organs would be allowed to make also additional checks before they override the absence of a valid key number and bring the station or card up to date again.

FIGURE 8 This shows an example for the LSI chip circuit block diagram. A chip of this type would be needed in an extension card for insertion in one of the the slots for extension functions, such as are common in personal computers. The following are the main features of the Chip:

The four clock phases needed to operate the circuit may be either on chip generated or supplied by the Computer (as fig. 8 indicates). The chip would also be used in the Service Center SC.There is a STORED KEY VERIFICATION AND KEY EXCHANGE MODULE (1). This group has four input lines (ROP, CK2, $\overline{\text{En}}$ and password .) and two output lines En & K . In connection with internet operation there may be at least one more input from outside the chip, when namely the output EN has to be delayed because of delays,in getting a connection completed or for whatever other reason. When the electric level at EN changes this indicates that verification and key exchange are satisfactorily completed, and, with everything else being ready the next phase can begin. - The ROP input to module 1 resets all internal bistables and occurs when power is switched on or shortly afterwards. The d-input is connected to the incoming signal line to enable the address reference for the encryption key held, to be read out . This last mentioned detail is not shown worked out in figure 8.

In practice, the circuit must satisfy the condition that external communication of keys must take place only in the encrypted form. The input CK2 provides the proper clock phase for the key exchange functions. The output K transfers to block 2 the new key before commencing the encryption and decryption functions. All encrypted incoming line signals are decrypted by gate 16.

The pseudo random key generator rotates the shift register 2 with every CK3 clock pulse. The programmable counter 4 is advanced with every $\overline{\text{CK3}}$ clock pulse. The bistable 23 is reset with every CK2 clock pulse. The programmable counter , after producing a carry output is loaded with the paralell output from the key generator at the time, that is between CK3 and the following CK2. The incoming or outgoing real data bits also have an effect on the constellation of the logic interconnections, block 3 in that the consecutive data bits are fed with the delay of one complete clock cycle to block 3.From this arrangement it follows that discovery of the clear text is not possible without the prior knowledge of the clear text, making discovery superfluous. Text generated in the P C is connected to a buffer register (17), or perhaps two such registers, via the terminal d_o The buffer fills until a signal F (full) is fed back to the computer. As the buffer clears due to passing on data to gate 14, the buffer register is filled up again from an overflow register in the computer itself.

The job of the pseudo random data generator, block 11, is to provide meaningless data bits to be fed to outlet 'd' via the gates 12 and 13 when $\overline{c}$ is high. The gate 14 admits data from the buffer 17 only when c is high. As the bistable outputs c and $\overline{c}$ are dependent on the rest of the algorithm, a quasi random mixture of real and fake data is produced at the d output when in the sending phase. When in the receiving phase, the scrambled mixture of real and random data bits is descrambled by gate 16. The remaining real data in the gate 16 output are channeled in the very beginning before the actual message transmission to gate 21 and to the d input to block 1 during the initial key checking and exchanging phase. The output from 21 feeds into a short shift register 7 which has paralell outputs for each of the bits it holds. These are applied to a static comparator 8 and compared bit by bit with an equal number of outputs from the register of block 2. As both the registers are shifted on the rising edge of CK3 but in opposite directions this has the effect of scanning and testing the registers as to the chance of hitting a seven bit (or 5-bit, etc.) combination where all the input bit comparisons are successful causing an output pulse by the strobing clock CK4 on AND gate 9 to trigger bistable 10. As the gate of 16b is enabled by $\overline{Q}$, with the disappearance of this high level the flow of encrypted nonsense data stops. A very similar arrangement in the Service Center SC also causes the flow of these data to stop and to connect the station A (Fig. 3)with station B directly via switch elements sw. From now on, encrypted data are meaningful text from A to B. Station B will from that moment on channel data received at d (Fig. 8) through gates 16 and 16a to the output interface d_i on the PCB whose adge contactors are plugged into the appropriate sockets inside the P C. When the workstation PC sends, an output SE is generated which disables the gate 16a. The computer can also generate a signal along chip input pwl (password line) to modify the encryption key as explained in connection with the comment on Figure 2.

Finally, the question should be addressed whether the present encryption system permits the communicating parties to engage in a dialogue. The answer is yes, messages may be sent in both directions with or without pause and there is no limit to the length of the message or of the dialogue.

Because of the nature of the encryptotion method which defies any form of systematic factoring of the encrypted text, it is unlikely that a free-lance hacker can be a threat to the described system in spite of the fact that the interchnages between the Client Computer (CC) and the Server Station (SSt) contain one element, the address information, in the clear. In a slightly better position are the expert engineers of the server stations which may have an insight into the precise moment when within the encrypted data flow various addresses are offered. In a very general way one may admit the possibility of a problem that may then arise.An alternative scheme would permit also the address code to be sent only in the encrypted form. According to our proposal, the Client Computers of a local region would have a special relationship with the Internet Secure Server station of that same region (SSt). The Client Computer (CC, Fig. 9) would when contacting the Server send to it its ID number.This number serves as an address in the Server station's memory bank which would contain the very same data as the Client station, namely

a chip serial nr. and / or the date of inauguration of the client chip (from an unalterable ROM).
the last entered encryption Key nr.
The last entered Preamble Delay nr. D_r
and in place of a revolving address code, an annual sequential entry serial nr.

Based on this information, the calling station may immediately begin with sending its own data in encrypted form which the receiving Server station would place into a comparator register, and if all these data are correct will automatically issue a new key number and preamble random delay number and the next sequential nr., in encrypted form using the old key, and the corresponding decrypted clear data are then placed into the memory of the Client Computer station. Its operator is requested to dial the distant station to which message material is to be sent. The dial number would pass through the encryption algorithm and therefor does not allow a third party to know which company or person will be connected. The first part of the dial code will call up the distant Server station (for example BBZ) and the number part will call up the particula CC, say 1500. When the latter responds, it sends its own ID number to the distant local Server station, and a similar comparison process as described above, is initiated. If this verifies that the correct CC station has been contacted, the new key (K_{n2}) given to the calling station is now also given to the called station. After this is verified, this is made known to the calling station, and a display invites its operator to proceed sending the intended material (text, drawings, voiced comment, etc).

The just described alternative logistics for a variable word length data transmission system, would blend well into telephone and internet based communication infra structures.

It is feasible that just one further step in this direction could be made by integrating the envisaged function of secure Server Stations with the location of telephone branch Exchanges (as indicated in Figure 10), This would be economical in installation costs,and could work fully automatically in the environment of an automatic switching system. This does not exclude the computerized electronic equipment being housed in a separate reinforced building. It would suffice to have that building in close vicinity to the said telephone Exchange station.

CLAIMS

1. An encryption and fully automatic key renewal system for confidential e-mail communication, comprising at least two e-mail stations linked to a communication system; the encryption and automatic key renewal system comprising:

a key generation centre (NKGC) for the generation of random keys for the use of said at least two e-mail stations;

means for the periodic renewal of the keys used by said at least two e-mail stations; and

means for scrambling or encrypting data to be transmitted, using said keys; and

local server stations which store and update said random keys generated in said key generation centre; characterised in that

said local server stations store said keys in a look-up table, each key being associated with an address code and each address code having associated data indicative of the age of said key at any time and to classify the age relative to the age of other keys in use at any given time; and

each said server station including means adapted to issue, prior to each confidential e-mail communication from said at least two e-mail stations, a new key to the sending e-mail station, as the key to be used by said station for scrambling or encrypting the data to be transmitted;

wherein said look-up table means stores a fixed number of encryption key numbers conjointly with their respective access addresses in a shift register-like memory structure wherein the said fixed group of key numbers and said addresses can be moved at quasi randomly arranged times from a younger to an older position the youngest position serving as an entrance point for a new number supplied by the said key generation centre, and the oldest number being relegated to an inactive and reserved position outside the said fixed number or group of encryption keys.

2. An encryption and fully automatic key renewal system as in claim 1, wherein the said at least two e-mail stations have means for encrypting and decrypting data including the key numbers themselves, comprising means for executing a key number replacement routine which accepts a new key number only on the basis of a successful completion of the replacement routine, the said routine being implemented prior to the transmission of a new key from the said Key Generation Centre, the said local Server Station (5), and the said e-mail stations.

3. An encryption and automatic key renewal system for confidential e-mail as in claim 1 or 2, comprising means for recognising the legitimacy of a server station by a calling e-mail station, comprising

(a) means for sending to the server station the address code associated with the e-mail station's encrypting key;

(b) means for using the address to assist the server station in obtaining the calling station's encryption key;

(c) the server station comprising equipment to encrypt the key encryption number with itself;

(d) the server station also comprising means to send the encrypted key to the e-mail station;

(e) the e-mail station comprising means for decrypting the received key, using its own key and placing the result into a comparator register, and means for determining if the compared numbers are equal for informing the server station accordingly.

4. An encryption and automatic key renewal system for

confidential e-mail as in claim 3, wherein in the case that the compared numbers are equal the server station is programmed to obtain from its storage means an alternative key number (K_c) from the currently stored key numbers, and to encrypt that new number with the key of the calling station, and wherein the latter is programmed upon receipt of the encrypted new key to decrypt said number and to place it into its key register in substitution of the number it had before.

5. An encryption and automatic key renewal system for confidential e-mail as in claim 3, wherein the server station (SC) also acts as an switchboard for connecting a calling station (A) to a requested receiving station (B), and wherein the server station consists of a computer section (COMP) and a twin structure which is equipped with two sets of encryption algorithm (algo) , two sets of switching controls, (LSA and LSB), and two sets of buffer memories (K_n) for holding key number, address codes and other relevant flags as supplied by the computer section (COMP).

6. An encryption and automatic key renewal system for confidential e-mail s in claim 5, wherein the said server station (SC) also contains a pseudo-random generator register (D_r) in order to generate quasi-data inputs of equal length simultaneously transmitted and encrypted by the said alternative key number (K_c) to the communicating stations (A, B) in order thereby to shift the starting conditions in the algorithms of the e-mail units for the real text to an undetectable point.

7. An encryption and automatic key renewal system for confidential e-mail as in claim 5 or 6, wherein the algorithms used for the encrypting process produce word-bit configurations consisting of more than 8 bits and less than 16 bits per word transmitted, and the bit

number per word is continually changing.

8. An encryption and automatic key renewals system for confidential e-mail as in claim 6, wherein the precise point in time for switching the communicating stations from the said initial meaningless random information is functionally defined by comparing the data flow in two registers, namely register (2) with that of register (7) whereby the data shift is prompted by the same clock phase (CK3) but occurs in opposite directions.

9. An encryption and automatic key renewal system for confidential e-mail as in any of the preceding claims, comprising

(a) a stored key verification and key exchange module (1),

(b) a Pseudo Random Key Generator (2),

(c) a system of logic circuit elements and interconnections between them

(d) a programmable counter (4)

(e) an open-ended shift register with parallel bit outputs (7)

(f) a pseudo-random Data Generator (11) for supplying surplus data bits

(g) a one clock-pulse delay circuit which delays real data bits (incoming and outgoing in affecting the state machine or algorithm status)

(h) a serial buffer system (18) for accepting work station data and to pass them to the algorithm in accordance with the instant state of the algorithm.

10. An encryption and automatic renewal system for confidential e-mail as in claim 9, wherein the said module (1) also contains mathematical processing means for adding or deducting a password from the operative key number in the key register of said module.

11. An encryption and automatic renewal system as claimed in any preceding claim, wherein said data to be encrypted is encrypted using a variable word length encryption system, wherein the data output from the encryption system comprises random data bits and real data bits, said real data bits being transmitted at a randomly varying rate, according to the key being used by said e-mail station.

12. In an encryption and fully automatic key renewal system, a key replacement routine comprises the steps of

in an automatic server station: receiving from a calling station a stored encryption key access address in clear text and in encrypted form the e-mail number of the party to be called,

based on said access address, identifying the encryption key which had been allocated to the calling station for its preceding confidential e-mail communication,

based on said identified key, the automatic server station encrypts the key by itself and adds a quasi random check number in encrypted form, and sends both to the calling station,

the calling station compares the decrypted received key with the one stored, and, if not identical, provides and indication thereof,

the automatic server station receives from the e-mail station the decrypted check number and compares it with the check number used before encrypting it, and, if not the same, will not proceed, and if the same, will decrypt the access number of the called station, and execute the call repeating the verification steps carried out with the calling station.

13. An encryption and automatic encryption key renewal system for confidential e-mail communication, comprising at least one e-mail station linked to a communication

system; said system comprising a pseudo-random data generator; characterised by a key generation system and an encryption circuit, said key generation system automatically providing said e-mail station with a new encryption key before each e-mail communication, and wherein the output of said pseudo-random data generator is mixed with the bit levels of outputs of said encryption circuit and with clear bit levels of said input data, according to said key, so as to diffuse any pattern such as may be recognised in the expanded data words.

14. An encryption and automatic key renewal system as claimed in claim 13, wherein the operation of said encryption circuit is continually influenced and modified

(a) by the parallel bit outputs of a revolving encryption key register, and

(b) by the clear bits of the data inputted to the encryption circuit for encryption or outputted from the encryption circuit after decryption.

15. An encryption and automatic key renewal system for confidential e-mail as claimed in any of claims 1 to 11, 13 or 14, wherein the encryption process is determined by an algorithm embodied in a microelectronic chip and wherein this process is not rigidly predetermined but continually influenced and modified

(a) by the parallel bit outputs of a revolving encryption key register, and

(b) by some but not all the clear bits of the data inputted to the said algorithm circuit for encryption or outputted from the said algorithm circuit after decryption.

16. An encryption and automatic key renewal system for confidential e-mail as characterised in claim 14,

wherein the functionality of the said microelectronic chip circuit is further influenced and modified

(c) by the configuration of a password entered by an operator at the sending and receiving stations in order to ensure that the transmitted text, picture or voice mail is faithfully reproduced only for those persons who are intended to know it.

17. An encryption and automatic key renewal system for confidential e-mail as in claim 15 wherein means for carrying out the encryption process includes a memory into which can be written only once, namely when a specific e-mail station is inaugurated and associated with a definite inauguration date, a definite serial number, and a definite name and a definite server station (SC), and wherein the said client computer (CC) details are also held in memory by the local server station (SSt) at an address number which is numerically identical with the ID of the CC concerned.

~~SHEET 6~~

~~STATEMENT WITH RESPECT TO BOX No IV~~
~~IN THIS DEMAND FOR INTERN. PREL. EXAMINATION.~~

~~As I have not yet received an International Search Report, on the other hand the time limit for submitting an amendment will expire within a few days, I have decided to request that a further subsidiery Claim be acknowledged to be part of my application for a European Patent, and be considered also by the international Patent Search Authority.~~

~~The additional Claim would be named Claim 14A and would read as follows:~~

14A. An encryption and autmatic key renewal system for confidential E-Mail as characterized in Claim 13 and 14 wherein the connections between certain of the paralell bit outputs of Key Register (Shift Register, SR, Figure 5) and the Logic Circuit (LC) are computer controlled and can thus be readily preset via a key board corresponding to a jointly agreed password by the communicating parties thereby ensuring that their respective algorithms operate in an unique synchronism.

~~The technical effect of this claim is similar to the arrangement characterised by Claim 9~~

CLAIMS

1. An encryption and automatic key renewal system for confidential E-Mail comprising at least one E-mail station or internet computer linked to a communication system
a national center for the generation of random keys for the use of said stations,
means for the scrambling or encrypting of data in said stations,
means for the periodic renewal of keys controling said scrambling means and local server centers which store and update the said random keys generated in said national center,
WHEREIN said keys shortly before they are delivered from the said Center become associated with one of a limited number of address codes, and
WHEREIN the number of the week within a year or some other flag data are attached to said address code that will readily permit the evaluation of the age of said key at any time and to classify its age relative to the age of other keys in use at a given time, and
WHEREIN FURTHER a server station when issuing the youngest number to an internet station will delete the oldest number from its current list of valid key numbers and utilise the former address code of that abandoned key for associating it with the youngest key (Fig. 7).

2. An encryption and automatic key renewal system for confidential E-mail as in CLAIM 1
WHEREIN the procedure for recognising the legitimacy of a Server Station by a calling E-mail station is as follows:
(a) sending to the server station the address code attached to its own encryption key
(b) the address must assist the server station in obtaining the calling station's encryption key
(c) The Server station equipment encrypts that key number by itself
(d) the Server station sends th encrypted key to the E-mail station
(e) the E-mail station decrypts using its own key and places the result into a comparator register
(f) If the compared numbers are equal, the E-mail equipment informs the Server sttaion accordingly (FIG. 7).

3. An encryption and automatic key renewal system for confidential E-mail as in Claim 2, WHEREIN in the case of receiving the OK signal the Server station is programmed to obtain from its computer section (COMP) an alternative key number (K_C) from the current valid list of key numbers, and to encrypt that new number with the key of the calling station, and wherein the latter is programmed upon receipt of the encrypted new key to decrypt siad number and to place it into its key register in substitution of the number it had before.

4. An encryption and automatic key renewal system for confidential E-mail as in Claim 3, WHEREIN the Server station (SC),Fig. 3, also acts as an Switchboard for connecting a calling station (A) to a requested receiving station (B), and WHEREIN the Server station consists of a twin structure which is equipped with two sets of encryption algorithm (algo), two sets of switching controls, (LSA and LSB), and two sets of buffer memories (K_n) for holding key number, address codes and other relevant flags as supplied by the computer section COMP.

5. An encryption and automatic key renewal system for confidential E-mail as in any preceding Claim WHEREIN the said twin sections of the said Server Center equipment (SC) also contains a pseudo-random generator register (D_r) in order to generate quasi-data inputs of equal length simultaneously transmitted and encrypted by the said K_C number to the communicating stations (A,B) in order thereby to shift the starting conditions in the algorithms of the E-mail units for the real text (see Fig. 4) to an undetectable point.

6. An encryption and automatic key renewal system for confidential E-mail as in claims 1 - 5 wherein the algorithms used for the encrypting process produce word-bit configurations consisting of more than 8 bits and less than 16 bits per word transmitted , and the bit number per word is continually changing.

7. An encryption and automatic key renewal system for confidential E-Mail as in CLAIM 5, WHEREIN the precise point in time for switching the communicating stations from the said initial meaningless random information (being received but not in its decrypted form outputted) is functionally defined by comparing the data flow in two registers, namely register 2 with that of register 7 whereby the data shift is prompted by the same clock phase (CK3) but occurs in opposite directions.

8. An encryption and automatic key renewal system for confidential E-Mail as in any of the preceding claims,
WHEREIN the main circuit groups of the integrated algorithm circuit (FIG. 8) comprises

(a) a stored key verification and key exchange module (1)
(b) a Pseudo Random Key Generator (2)
(c) a system of logic circuit elements and interconnections between them
(d) a programmable :ounter (4)
(e) an open-ended shift register with paralell bit outputs (7)
(f) a pseudorandom Data Generator (11) for supplying surplus data bits
(g) a one clock-pulse delay circuit which delays real data bits (incoming and outgoing in affecting the state machine or algorithm status
(h) a serial buffer system 17 for accepting work station data and to pass them to the algorithm in accordance with the instant state of the algorithm.

9. An encryption and automatic renewal system for confidential E-Mail as in Claim 8, wherein the said circuit block (1) also contains mathematical processing means, for example for adding or deducting a Pass Word from the operative Key number in the key register of said module.

10. An encryption and automatic key renewal system for confidential E-Mail as in any of the aforegoing claims, and / or as shown and described in the accompanying drawings and the 'Specification.

11. An encryption and automatic encryption key renewal system for confidential E-Mail wherein the output of the said pseudo-random data generator is mixed with the bit levels of other outputs of the encryption circuit or with the clear bit levels of the data flow so as to diffuse any pattern such as may be recognised in the expanded data words.

12. An encryption and automatic key renewal system for confidential E-Mail wherein the basic functionality of the said algorithm circuit is continually influenced and modified

(a) by the paralell bit outputs of a revolving encryption key register

and (b) by the clear bits of the data inputted to the algorithm circuit for encryption or outputted from the algorithm circuit after decryption.

13. An encryption and automatic key renewal system for confidential E-Mail essentially as characterised in Claim 1 wherein the functionality of the encryption process is broadly determined by an, partly in special hardware executed, algorithm and embodied in a microelectronic chip and wherein this functionality is not rigidly predetermined but continually influenced and modified

(a) by the paralell bit outputs of a revolving encryption key register, and

(b) by some but not all the clear bits of the data inputted to the said algorithm circuit for encryption or outputted from the said algorithm circuit after decryption.

14. An encryption and automatic key renewal system for confidential E-Mail as characterised in Claim 13 wherein the functionality of the said microelectronic chip circuit is further influenced and modified

(c) by the configuration of a password entered by an operator at the sending and receiving stations in order to ensure that the transmitted text, picture, or voice mail is faithfully reproduced only for those persons who are intended to know it.

15. An encryption and automatic key renewal system for confidential E-Mail as in Claim 13 wherein the in hardware represented portion of the encryption algorithm also contains memory into which can be written only once, namely when a specific E-Mail station is inaugurated and associated with a definite inauguration date, a definite serial number, and a definite name and a definite Server Station (SSt), and wherein the said Client Computer (CC) details are also held in memory by the local Server Station (SSt) at an address numvber which is numerically identical with the ID of the CC concerned.

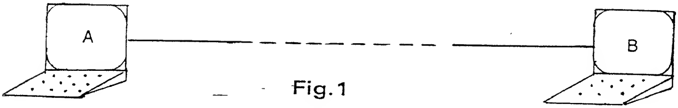


Fig.1

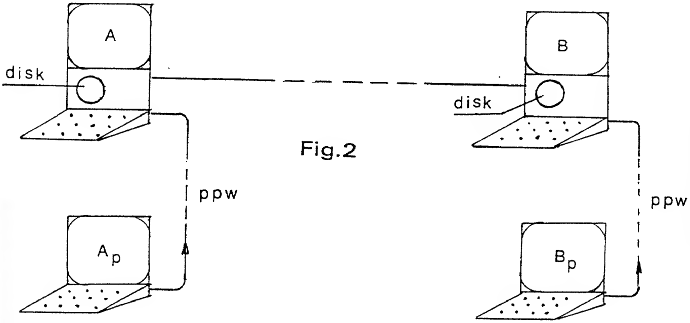


Fig.2

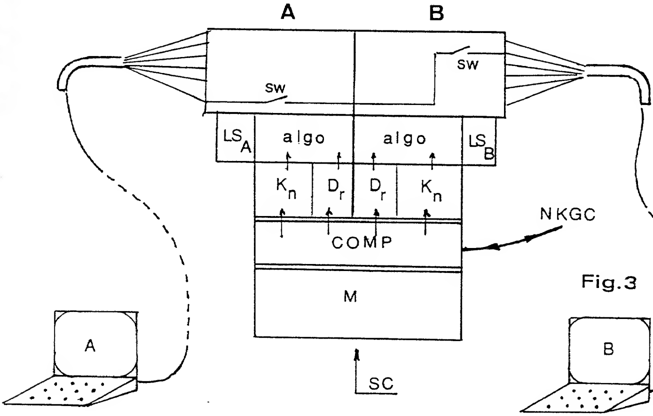
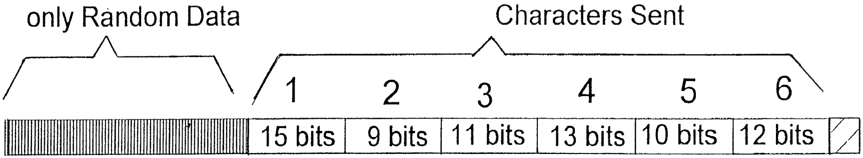


Fig.3

The three modifying components acting together, produce:



The scrambled variable word length
data constitute a single message
string defying analysis

Fig.4

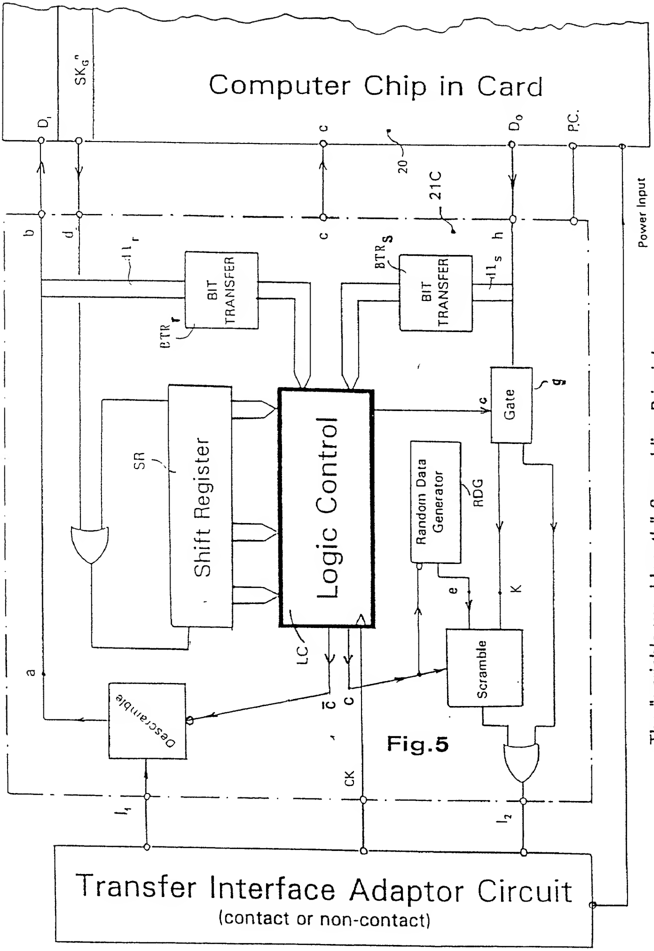


Fig.5

The "variable-word-length" Scrambling Principles
(functional block diagram)

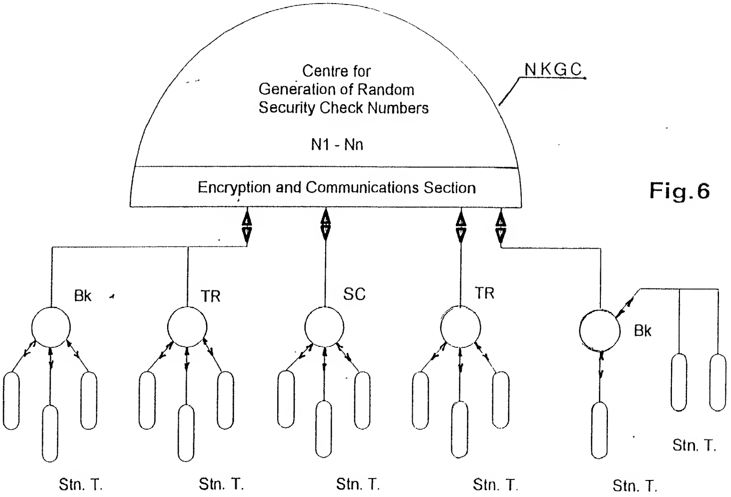


Fig.6

Hierarchical distribution pattern

Bk = bank
TR = transport terminal
Stn.T. = message station terminal

Abandoned Numbers	semi-active numbers					active numbers					Nascent numbers
	10	*9*	*8*	*7*	*6*	*5*	*4*	*3*	*2*	*1*	← – – *address register*
	N_{10}	N_9	N_8	N_7	N_6	N_5	N_4	N_3	N_2	N_1	←—— **number register**
	9	*8*	*7*	*6*	*5*	*4*	*3*	*2*	*1*	*10*	← – –
	N_9	N_8	N_7	N_6	N_5	N_4	N_3	N_2	N_1	N_{11}	←——
	8	*7*	*6*	*5*	*4*	*3*	*2*	*1*	*10*	*9*	← – –
	N_8	N_7	N_6	N_5	N_4	N_3	N_2	N_1	N_{11}	N_{12}	←——
	7	*6*	*5*	*4*	*3*	*2*	*1*	*10*	*9*	*8*	
	N_7	N_6	N_5	N_4	N_3	N_2	N_1	N_{11}	N_{12}	N_{13}	
	6	*5*	*4*	*3*	*2*	*1*	*10*	*9*	*8*	*7*	
	N_6	N_5	N_4	N_3	N_2	N_1	N_{11}	N_{12}	N_{13}	N_{14}	
	5	*4'*	*3*	*2*	*1*	*10*	*9*	*8*	*7*	*6*	
	N_5	N_4	N_3	N_2	N_1	N_{11}	N_{12}	N_{13}	N_{14}	N_{15}	
	4	*3*	*2*	*1*	*10*	*9*	*8*	*7*	*6*	*5*	
	N_4	N_3	N_2	N_1	N_{11}	N_{12}	N_{13}	N_{14}	N_{15}	N_{16}	
	3	*2*	*1*	*10*	*9*	*8*	*7*	*6*	*5*	*4*	
	N_3	N_2	N_1	N_{11}	N_{12}	N_{13}	N_{14}	N_{15}	N_{16}	N_{17}	
	2	*1*	*10*	*9*	*8*	*7*	*6*	*5*	*4*	*3*	
	N_2	N_1	N_{11}	N_{12}	N_{13}	N_{14}	N_{15}	N_{16}	N_{17}	N_{18}	
	1	*10*	*9*	*8*	*7*	*6*	*5*	*4*	*3*	*2*	
	N_1	N_{11}	N_{12}	N_{13}	N_{14}	N_{15}	N_{16}	N_{17}	N_{18}	N_{19}	

Fig.7 - Surveying the position changes and new entries of check numbers during ten consecutive time periods

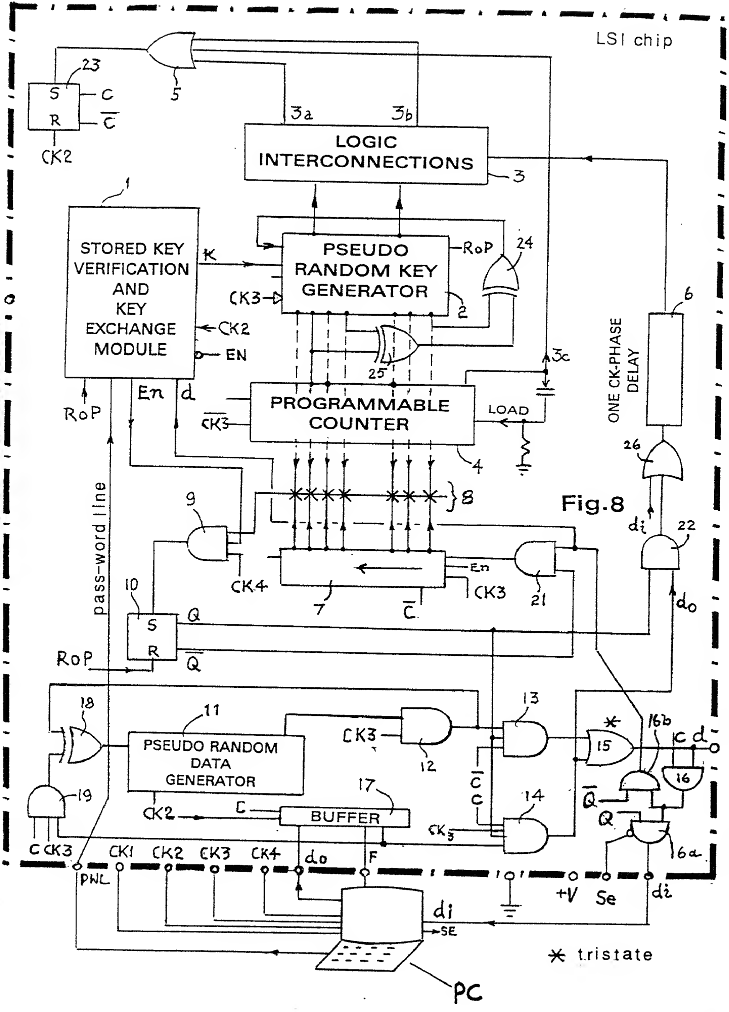

LSI chip
23
S
R
C
C̄
CK2
5
3a
3b
LOGIC INTERCONNECTIONS
3
1
STORED KEY VERIFICATION AND KEY EXCHANGE MODULE
K
PSEUDO RANDOM KEY GENERATOR
RoP
24
CK3
2
CK2
EN
25
3c
6
ONE CK-PHASE DELAY
RoP
En
d
PROGRAMMABLE COUNTER
LOAD
CK3
4
26
8
9
pass-word line
CK4
7
En
CK3
21
C̄
di
22
do
10
S
R
Q
Q̄
RoP
18
11
PSEUDO RANDOM DATA GENERATOR
13
CK3
12
*
15
16b
c
d
16
C̄
C
14
Q̄
Q
19
CK2
C
17
BUFFER
CK3
6a
C CK3
CK1
CK2
CK3
CK4
do
F
PWL
+V
Se
di
di
SE
PC
* tristate

Fig.8

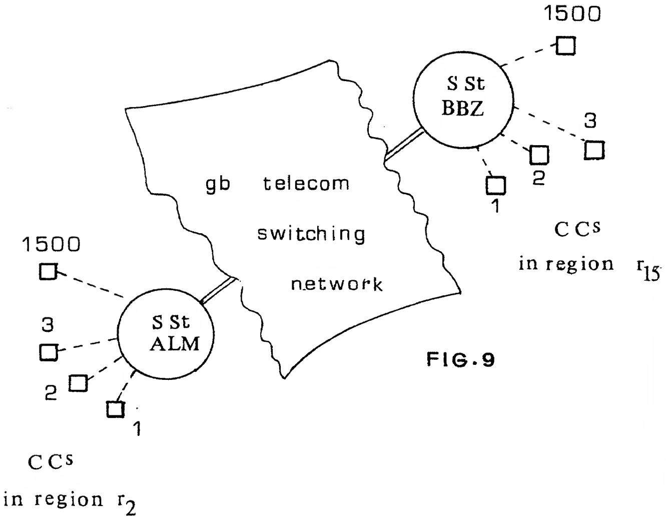

1500
S St
BBZ
3
2
1
C Cs
in region r15
gb telecom
switching
network
1500
3
S St
ALM
2
1
C Cs
in region r2

FIG.9

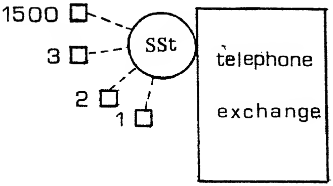

1500
3
2
1
SSt
telephone
exchange

FIG.10

Type a plus sign (+) inside this box → [+]

0010/PTO Rev. 6/95	U.S. Department of Commerce Patent and Trademark Office	Attorney Docket	HALJW/102/PC/US
		First Named Inventor	John Wolfgang Halpern
		COMPLETE IF KNOWN	
DECLARATION		Application Number	09/787,575
☐ Declaration Submitted with Initial Filing	☒ Declaration Submitted after Initial Filing	Filing Date	March 19, 2001
		Group Art Unit	
		Examiner Name	

As an above named inventor, I hereby declare that:

My residence, post office address, and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

A Data Encryption System for Internet Communication

(Title of the Invention)

the specification of which

☐ is attached hereto

OR

☒ was filed on (MM/DD/YYYY) September 24, 1998 as United States Application or PCT International Application Number PCT/GB98/02881 and was amended on (MM/DD/YYYY) March 19, 2001 (if applicable).

I hereby state that I have reviewed and understood the contents of the above-identified specification, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in Title 37 Codes of Federal Regulations, §1.56.

I hereby claim foreign priority under Title 35, United States Code § 119 (a)-(d) or § 365 (b) of any foreign application(s) for patent or inventor's certificate, or § 365 (a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or of any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application Numbers	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Copy Attached Yes	Copy Attached No
9720478.8	Great Britain	September 25, 1997	☐	☐	☒
9820824.2	Great Britain	September 24, 1998	☐	☐	☒
			☐	☐	☐
			☐	☐	☐

☐ Additional foreign application numbers are listed on a supplemental priority sheet attached hereto:

I hereby claim the benefit under Title 35, United States Code § 119 (e) of any United States provisional application(s) listed below:

Application Number(s)	Filing Date (MM/DD/YY)	
		☐ Additional provisional application numbers are listed on a supplemental priority sheet attached hereto.

DECLARATION	Page 2

I hereby claim the benefit under Title 35, United States Code §120 of any United States application(s), or §365(c) of any PCT International application designating the United States of America, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of Title 35, United States Code §112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Title Code of Federal Regulations §1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application.

U.S. Parent Application Number	PCT Parent Number	Parent Filing Date (MM/DD/YYYY)	Parent Patent Number (if applicable)

□ Additional U.S. or PCT International application numbers are listed on a supplementary priority sheet attached hereto:

As a named inventor, I hereby appoint the registered practitioners associated with the Customer Number provided below to prosecute this application and to transact all business in the Patent and Trademark Office therewith, and direct that all correspondence be addressed to that Customer Number:

Firm Name: **Alix, Yale & Ristas, LLP** Customer Number: 002543

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment or both under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Name of Sole or First Inventor □ A petition has been filed for this unsigned inventor

Given Name	John	Middle Initial	W.	Family Name	Halpern	Suffix			
Inventor's Signature				Date	2002/03/09				
RESIDENCE: City	Ingram Crescent	State	West Hove	Country	United Kingdom GBX	Citizenship	United Kingdom		
POST OFFICE ADDRESS	15 Jordan Court								
City	Ingram Crescent	State	West Hove	Zip	BN3 5NU	Country	United Kingdom	Applicant Authority	

Name of Additional Joint Inventor, if any: □ A petition has been filed for this unsigned inventor

Given Name		Middle Initial		Family Name		Suffix			
Inventor's Signature				Date					
RESIDENCE: City		State		Country		Citizenship			
POST OFFICE ADDRESS									
City		State		Zip		Country		Applicant Authority	

□ Additional inventors are being named on supplemental sheet(s) attached hereto.